ABSTRACT

In general, a method of securely transmitting data features an operation of authenticating a user of a platform during a Basic Input/Output System (BIOS) boot process. In response to authenticating the user, a first keying material is released from a token communicatively coupled to the platform. The first keying material is combined with a second keying material internally stored within the platform in order to produce a combination key. This combination key is used to decrypt a second BIOS area to recover a second segment of BIOS code.